UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,121	04/27/2001	Bjorn Markus Jakobsson	45-1-1	1053

7590 12/14/2006

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,121	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-22 and 24-28* is/are rejected.

7)☒ Claim(s) *9,23* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 14, 2006. Claims 1-28 are currently pending consideration.

Response to Arguments

2. Applicant's arguments with respect to claims 1-28 have been considered but are moot in view of the new ground(s) of rejection.

Allowable Subject Matter

3. Claims 9 and 23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6, 8, 10-12, 14-20,22, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (U.S. Patent 6,257,638) in view of Abramson, "Control Strategies for Two-Player Games" in view of Aiello et al. (U.S. Patent 6,496,808).

Regarding claim 1, Walker discloses:

A method for performing secure information processing operations utilizing a plurality of processing devices, the method comprising the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54);

wherein the interaction comprises a number of consecutive rounds of one or more decisions by each of the first participant and the second participant (column 11 lines 38-50, column 15 lines 29-53).

Walker does not explicitly disclose wherein the interaction is characterized by a first tree structure associated with the first participant and a second tree structure associated with a second participant, with each subset of nodes comprising a block of data which determines randomness of a corresponding round. Abramson discloses a mathematical model which is called a game tree which the two-player zero sum game is based (page 137: column 2, 2nd paragraph). Each participant has a tree structure associated with them, where each tree has moves for each round of play (page 152: column 2, 2nd paragraph). The tree structures have a set of random variables drawn from a distribution function, which provides rounds (leaves) with randomness (page 152: column 2, 2nd paragraph). Walker and Abramson are analogous arts in that both are related to gaming between more than one participant. It would have been obvious to

one of ordinary skill in the art at the time of invention to use the tree structures present in the computer games delineated by Abramson in the remote gaming system of Walker, so that multiple game types can be supported, including the games which use the zero sum principle (Abramson: page 137, column 2, paragraph 2).

The combination of Walker-Abramson does not explicitly disclose that at least a subset of nodes are decision preimage values that encode possible decisions to be made in the interaction. Aiello discloses a game in which participants have a plurality of consecutive moves or decisions, in which each decision is subject to a hash function (preimage) (column 5 lines 20-43). It would have been obvious to one of ordinary skill in the art to provide these preimage (hash) values that encode the decisions in the gaming system of Walker-Abramson so that the house and the user can be assured that the game is proceeding fairly and that no cheating is taking place (Aiello: column 2 lines 27-22).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the receiving and sending steps are repeated one or more times in accordance with specifications of the particular interaction (column 10 lines 42-46, column 13 lines 25-38, column 13 line 43 – column 14 line 7).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the first processing device comprises at least one lightweight device configured to communicate over a network with the second processing device (column 8 lines 33-40).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction in which the first participant corresponds to a player and the second participant corresponds to a casino (column 8 lines 23-33).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Walker discloses:

The method of claim 4 wherein the first processing device comprises a lightweight processing device associated with the player and the second processing device comprises at least one server associated with the casino (column 8 lines 23-47)

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction involving two or more players in which the first participant corresponds to a first player and the second participant corresponds to a second player

(column 8 lines 23-47, column 11 lines 38-50).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure digital signature exchange interaction in which the first participant corresponds to a first party to the digital signature exchange and the second participant corresponds to a second party to the digital signature exchange (column 5 line 56 – column 6 line 20)

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein security of the particular interaction is based at least in part on a secure probabilistic symmetric cipher (E, D) having semantic security operating in conjunction with a one-way hash function h for which collisions are intractable to find, and a commitment function C, wherein the commitment function C provides the public verifiability of designated portions of the interaction (column 5 line 56 – column 6 line 20).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the interaction is configured such that if at least one of the first and second processing devices is disconnected during the interaction,

the interaction may upon reconnection of the device be continued from a designated point at or prior to the disconnection without the participants being able to alter any partial results of the interaction attributable to a portion of the interaction up to the designated point (column 4 lines 10-21, column 6 lines 43-54).

Claim 11 is rejected as applied above in rejecting claim 4. Furthermore, Walker discloses:

The method of claim 4 wherein the secure mobile gaming interaction comprises at least one game played by the player with the casino, the game comprising a number of consecutive rounds of one or more moves by each of the player and the casino, each of the rounds allowing the player and the casino to commit to at least one decision (column 11 lines 38-50, column 15 lines 29-53).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Walker discloses:

The method of claim 11 wherein the game is characterized by a player game tree structure associated with the player and a casino game tree structure associated with the casino, each of the game tree structures comprising a plurality of nodes, each of at least a subset of the nodes comprising a block of data that determines randomness contributed to a corresponding round of the game by the corresponding player or casino, wherein associated with each of at least a subset of the game nodes are decision preimage values that encode possible decisions to be made in the game

(column 11 lines 8-30).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the setup procedure comprises at least the following steps:

(a) the player selecting n random numbers d.sub.il, . . . , d.sub.in, for each node i of the player game tree structure, and a random number r.sub.i uniformly at random for each node, wherein each node i corresponds to a particular round of the game;

(b) the player computing for each node i a corresponding game node value game.sub.i=<h(D.sub.il, . . . D.sub.in), R.sub.i>, where D.sub.ij=h(d.sub.ij), R.sub.i=C(r.sub.i), h denotes a hash function, C denotes a commitment function, and preimage.sub.i=(d.sub.il, . . . , d.sub.in, r.sub.i,) denotes a decision preimage value for game.sub.i;

(c) the player computing for each node i a value which is a function of one or more of: (i) values associated with one or more of its children nodes; (ii) its corresponding game node value game.sub.1; and (iii) a descriptor that identifies the game type;

(d) both the player and the casino storing information of the form agreement .sub.(casino,player) comprising a root value of the player game tree structure, a root value of the casino game tree structure, a hash value on a game function .function..sub.game, and associated digital signatures by the player and the casino.

Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the secure mobile gaming interactions are implemented in accordance with a game-playing protocol comprising at least the following steps:

(a) the player initiating the game by sending a value r.sub.player,cnt the casino, where cnt corresponds to a counter (column 12 line 56 – column 13 line 38));

(b) the casino verifying that r.sub.player,cnt is a correct preimage to R.sub.player,cnt , and halting the protocol if it is not the correct preimage (column 11 lines 8-30, column 12 line 56 – column 13 line 38);

(c) the casino and the player taking turns making moves in which the casino sends to the player decision preimages encoding its move, the player is presented with one or more corresponding choices via an interface at the first processing device, and a given choice selected by the player is translated into one or more preimages that are subsequently sent to the casino (column 11 lines 8-30, column 15 lines 39-64);

(d) step (c) being repeated one or more times in accordance with the rules of the game (column 15 lines 39-64);

(e) the casino sending a value r.sub.casino,cnt to the player, which is verified correspondingly by the player (column 6 line 43 – column 7 line 23);

(f) evaluating a game function .function..sub.game on the disclosed portions of the player and casino preimages, presenting a corresponding output to the player and

the casino, and sending appropriate payment transcripts to at least one financial institution (column 7 lines 23-35); and

(g) the player and the casino each updating the counter cnt, along with other state information associated with a current state of the game (column 6 line 43 – column 7 line 23).

Regarding claim 15, Walker discloses:

An apparatus for use in performing secure information processing operations, the apparatus comprising:

a memory (column 2 lines 32-39); and

a processor coupled to the memory, the memory and processor being elements of a first processing device associated with a first participant, the processor being operative:

(i) to perform a setup procedure to permit interactions of a designated type to be carried out between the first participant and a second participant associated with at least a second processing device (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

(ii) to initiate a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

(iii) receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

(iv) sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54);

wherein the interaction comprises a number of consecutive rounds of one or more decisions by each of the first participant and the second participant (column 11 lines 38-50, column 15 lines 29-53).

Walker does not explicitly disclose wherein the interaction is characterized by a first tree structure associated with the first participant and a second tree structure associated with a second participant, with each subset of nodes comprising a block of data which determines randomness of a corresponding round. Abramson discloses a mathematical model which is called a game tree which the two-player zero sum game is based (page 137: column 2, 2nd paragraph). Each participant has a tree structure associated with them, where each tree has moves for each round of play (page 152: column 2, 2nd paragraph). The tree structures have a set of random variables drawn from a

distribution function, which provides rounds (leaves) with randomness (page 152: column 2, 2nd paragraph). Walker and Abramson are analogous arts in that both are related to gaming between more than one participant. It would have been obvious to one of ordinary skill in the art at the time of invention to use the tree structures present in the computer games delineated by Abramson in the remote gaming system of Walker, so that multiple game types can be supported, including the games which use the zero sum principle (Abramson: page 137, column 2, paragraph 2).

The combination of Walker-Abramson does not explicitly disclose that at least a subset of nodes are decision preimage values that encode possible decisions to be made in the interaction. Aiello discloses a game in which participants have a plurality of consecutive moves or decisions, in which each decision is subject to a hash function (preimage) (column 5 lines 20-43). It would have been obvious to one of ordinary skill in the art to provide these preimage (hash) values that encode the decisions in the gaming system of Walker-Abramson so that the house and the user can be assured that the game is proceeding fairly and that no cheating is taking place (Aiello: column 2 lines 27-22).

Regarding claim 27, Walker discloses:

An article of manufacture comprising a machine-readable storage medium for storing one or more programs for use in performing secure information processing operations utilizing a plurality of processing devices, wherein the one or more programs when executed implement the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54);

wherein the interaction comprises a number of consecutive rounds of one or more decisions by each of the first participant and the second participant (column 11 lines 38-50, column 15 lines 29-53).

Walker does not explicitly disclose wherein the interaction is characterized by a first tree structure associated with the first participant and a second tree structure associated with a second participant, with each subset of nodes comprising a block of data which determines randomness of a corresponding round. Abramson discloses a mathematical model which is called a game tree which the two-player zero sum game is based (page 137: column 2, 2nd paragraph). Each participant has a tree structure associated with them, where each tree has moves for each round of play (page 152: column 2, 2nd paragraph). The tree structures have a set of random variables drawn from a distribution function, which provides rounds (leaves) with randomness (page 152: column 2, 2nd paragraph). Walker and Abramson are analogous arts in that both are related to gaming between more than one participant. It would have been obvious to one of ordinary skill in the art at the time of invention to use the tree structures present in the computer games delineated by Abramson in the remote gaming system of Walker, so that multiple game types can be supported, including the games which use the zero sum principle (Abramson: page 137, column 2, paragraph 2).

The combination of Walker-Abramson does not explicitly disclose that at least a subset of nodes are decision preimage values that encode possible decisions to be made in the interaction. Aiello discloses a game in which participants have a plurality of consecutive moves or decisions, in which each decision is subject to a hash function

(preimage) (column 5 lines 20-43). It would have been obvious to one of ordinary skill in the art to provide these preimage (hash) values that encode the decisions in the gaming system of Walker-Abramson so that the house and the user can be assured that the game is proceeding fairly and that no cheating is taking place (Aiello: column 2 lines 27-22).

Regarding claim 28, Walker discloses:

A method for performing secure information processing operations utilizing a plurality of processing devices including at least a first processing device associated with a first participant and a second processing device associated with a second participant, the method comprising the steps of:

receiving from the first processing device in the second processing device designated initiation information initiating a particular interaction between the first participant and the second participant, the particular interaction being configured based at least in part on one or more results of a setup procedure, the setup procedure being performed by the first participant associated with the first processing device and permitting the particular interactions to be carried out between the first participant and the second participant (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

sending as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10); and

receiving as part of the interaction additional information sent from the first processing device to the second processing device based at least in part on the response information (column 5 line 56 – column 6 line 20);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54);

wherein the interaction comprises a number of consecutive rounds of one or more decisions by each of the first participant and the second participant (column 11 lines 38-50, column 15 lines 29-53).

Walker does not explicitly disclose wherein the interaction is characterized by a first tree structure associated with the first participant and a second tree structure associated with a second participant, with each subset of nodes comprising a block of data which determines randomness of a corresponding round. Abramson discloses a mathematical model which is called a game tree which the two-player zero sum game is based (page 137: column 2, 2nd paragraph). Each participant has a tree structure associated with them, where each tree has moves for each round of play (page 152: column 2, 2nd paragraph). The tree structures have a set of random variables drawn from a distribution function, which provides rounds (leaves) with randomness (page 152: column 2, 2nd paragraph). Walker and Abramson are analogous arts in that both are related to gaming between more than one participant. It would have been obvious to one of ordinary skill in the art at the time of invention to use the tree structures present

in the computer games delineated by Abramson in the remote gaming system of Walker, so that multiple game types can be supported, including the games which use the zero sum principle (Abramson: page 137, column 2, paragraph 2).

The combination of Walker-Abramson does not explicitly disclose that at least a subset of nodes are decision preimage values that encode possible decisions to be made in the interaction. Aiello discloses a game in which participants have a plurality of consecutive moves or decisions, in which each decision is subject to a hash function (preimage) (column 5 lines 20-43). It would have been obvious to one of ordinary skill in the art to provide these preimage (hash) values that encode the decisions in the gaming system of Walker-Abramson so that the house and the user can be assured that the game is proceeding fairly and that no cheating is taking place (Aiello: column 2 lines 27-22).

5. Claims 16-20, and 22-26 are apparatus claims analogous to the method claims 1-6, 8-12, and 14 rejected above, and therefore, are rejected following the same reasoning.

6. Claims 7, 13, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,527,638) in view of Abramson, "Control Strategies for Two-Player Games" in view of Aiello et al. (U.S. Patent 6,496,808) in view of Takaragi et al. (U.S. Patent No. 5,018,196).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1. Walker does not explicitly disclose that the particular interaction comprises secure contract signing interaction in which the first participant corresponds to a first party to the contract and the second participant corresponds to a second party to the contract. Takaragi discloses a system wherein two parties exchange preliminary digital signatures, and then agree to a contract by exchanging their formal digital signatures with each other, and further, if there are problems, a third party can decode the signatures submitted by the transaction parties, and use a hash total of the contract, to verify the transaction (Abstract, column 4 lines 14-47). Walker and Takaragi are analogous arts in that both exchange authenticable messages with digital signatures. Walker disclose a system of cashing out, purchasing more gambling credit, via a communication with the wagering establishment (casino). This procedure requires the exchange of authenticable messages as disclosed by Walker. It would have been obvious that these authenticable messages could compose of a contract which has to be digitally signed by each party. This would allow a third party to intervene if a problem arises, so that "neither of the transacting parties can deny that it has approved formally the transaction, if the other party submits its digital signature as evidence" (column 5 lines 7-14). This would be important in the transactions involved in Walker which involve monetary funds. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the contract signing method of

Takaragi with the system of verifying the exchange of funds of Walker, to insure the liability of both parties when exchanging monetary funds.

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the setup procedure comprises at least the following steps:

(a) the player selecting n random numbers d.sub.il, . . . , d.sub.in, for each node i of the player game tree structure, and a random number r.sub.i uniformly at random for each node, wherein each node i corresponds to a particular round of the game (column 15 lines 39-64);

(b) the player computing for each node i a corresponding game node value game.sub.i=<h(D.sub.il, . . . D.sub.in), R.sub.i>, where D.sub.ij=h(d.sub.ij), R.sub.i=C(r.sub.i), h denotes a hash function, C denotes a commitment function, and preimage.sub.i=(d.sub.il, . . . , d.sub.in, r.sub.i,) denotes a decision preimage value for game.sub.i (column 5 line 56 – column 6 line 20, column 11 lines 10-30);

(c) the player computing for each node i a value which is a function of one or more of: (i) values associated with one or more of its children nodes; (ii) its corresponding game node value game.sub.1; and (iii) a descriptor that identifies the game type (column 5 line 56 – column 6 line 20, column 11 lines 10-30);

Walker does not explicitly disclose that the player and the casino store an agreement (casino, player) comprising a root value of the player game tree structure, a

root value of the casino game tree structure, a hash value on a game function, and associated digital signatures by the player and the casino. Takaragi discloses a system wherein two parties exchange preliminary digital signatures, and then agree to a contract by exchanging their formal digital signatures with each other, and further, if there are problems, a third party can decode the signatures submitted by the transaction parties, and use a hash total of the contract, to verify the transaction (Abstract, column 4 lines 14-47). Walker and Takaragi are analogous arts in that both exchange authenticable messages with digital signatures. Walker disclose a system of cashing out, purchasing more gambling credit, via a communication with the wagering establishment (casino). This procedure requires the exchange of authenticable messages as disclosed by Walker. It would have been obvious that these authenticable messages could compose of a contract, which has to be digitally signed by each party. This would allow a third party to intervene if a problem arises, so that "neither of the transacting parties can deny that it has approved formally the transaction, if the other party submits its digital signature as evidence" (column 5 lines 7-14). This would be important in the transactions involved in Walker which involve monetary funds. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the contract signing method of Takaragi with the system of verifying the exchange of funds of Walker, to insure the liability of both parties when exchanging monetary funds.

7. Claim 21 is an apparatus claim analogous to the method claim of claim 13, and therefore, is rejected following the same reasoning.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
12/08/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100